Claims

What is claimed is:

1. A method for protection of computer assets from unauthorized access comprising the steps of:

receiving in a protection engine, an interface control command;

determining whether the interface control command introduces a security risk;

when the interface control command introduces a security risk, determining a state of a switch;

when the state of the switch is a protected state, inhibiting execution of the interface control command; and

when the state of the switch is an unprotected state, allowing execution of the interface control command.

2. The method of claim 1 wherein the step of inhibiting execution of the interface control command further includes the step of:

providing an indication that the execution of the interface control command was inhibited.

3. The method of claim 1 further comprising the step of:

changing the state of the switch to the protected state when a timeout duration has elapsed.

4. The method of claim 1 further comprising the steps of:

determining when the execution of the interface control command has been completed; and

when the execution of the interface control command has been completed, changing the state of the switch to the protected state.

5. The method of claim 1. wherein the step of determining the state of a switch includes the step of:

determining the state of an electrical switch (physical switch).

6. The method of claim 1 wherein the step of determining the state of a switch includes the step of:

determining the state of a software-based switch.

7. The method of claim 6 wherein the step of determining the state of the software-based switch includes the step of:

using cryptographic techniques to determine the state of the software-based switch.

8. The method of claim 1 wherein the step of allowing execution of the interface control command further comprises the step of:

allowing data to be written to a hard disk drive.

9. The method of claim 8 wherein the step of allowing data to be written to a hard disk drive comprises the step of:

allowing data to be written to a boot sector of the hard disk drive.

10. The method of claim 8 wherein the step of allowing data to be written to a hard disk drive comprises the step of:

allowing data to be written to a file allocation table of the hard disk drive.

11. The method of claim 1 wherein the step of allowing execution of the interface control command further comprises the step of:

allowing data to be written to a floppy disk drive.

12. The method of claim 1 wherein the step of allowing execution of the interface control command further comprises the step of:

allowing data to be written to a BIOS memory.

13. The method of claim 1 wherein the step of allowing execution of the interface control command further comprises the step of:

allowing data to be written to a parallel port.

14. The method of claim 1 wherein the step of allowing execution of the interface control command further comprises the step of:

allowing data to be written to a serial port.

15. The method of claim 14 wherein the step of allowing data to be written to a serial port further comprises the step of:

allowing data to be written to a universal serial bus (USB).

16. The method of claim 14 wherein the step of allowing data to be written to a serial port further comprises the step of:

allowing data to be written to an IEEE-1394 interface.

17. The method of claim 13 wherein the step of allowing execution of the interface control command further comprises the step of:

allowing data to be written to a flash memory device.

18. The method of claim 13 wherein the step of allowing execution of the interface control command further comprises the step of:

allowing data to be written to a thermal management controller.

19. The method of claim 1 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command is a hard disk drive formatting command.

20. The method of claim 19 wherein the step of determining whether the interface control command is the hard disk drive formatting command further comprises the step of:

determining whether the interface control command is a boot sector write command.

21. The method of claim 1 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command is a program file write command.

22. The method of claim 21 wherein the step of determining whether the interface control command is a program file write command further comprises the steps of:

obtaining a file extension from the interface control command;

determining whether the file extension is an executable file extension.

23. The method of claim 22 wherein the step of determining whether the file extension is an executable file extension further comprises the step of:

determining whether the file extension is one of a exe extension, a com extension, a bat extension, or a bin extension.

24. The method of claim 1 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command changes a file attribute, the file attribute enabling or disabling execution of a file corresponding to the file attribute.

25. The method of claim 1 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command disables a thermal management subsystem.

26. The method of claim 25 wherein the step of determining whether the interface control command disables a thermal management subsystem comprises the step of:

determining whether the interface control command disables a fan.

27. The method of claim 1 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command is a write command to write to a system firmware (BIOS).

28. The method of claim 1 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command is a write command to write to a parallel port.

29. The method of claim 1 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command is a write command to write to a serial port.

30. The method of claim 29 wherein the step of determining whether the interface control command interface control command is a write command to write to a serial port comprises the step of:

determining whether the interface control command is a write command to write to a universal serial bus (USB).

31. The method of claim 29 wherein the step of determining whether the interface control command interface control command is a write command to write to a serial port comprises the step of:

determining whether the interface control command is a write command to write to an IEEE-1394 interface.

32. The method of claim 1 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command is a write command to write to a flash memory device.

33. A method for protection of computer assets from unauthorized access comprising the steps of:

receiving in a protection engine, an interface control command;

determining whether the interface control command introduces a security risk;

when the interface control command introduces a security risk, determining whether of a source of the interface control command is authentic;

when the source of the interface control command is not authentic, inhibiting execution of the interface control command; and

when the source of the interface control command is authentic, allowing execution of the interface control command.

34. The method of claim 33 wherein the step of inhibiting execution of the interface control command further includes the step of:

providing an indication that the execution of the interface control command was inhibited.

35. The method of claim 33 wherein the step of allowing execution of the interface control command further comprises the step of:

allowing data to be written to a hard disk drive.

36. The method of claim 35 wherein the step of allowing data to be written to a hard disk drive comprises the step of:

allowing data to be written to a boot sector of the hard disk drive.

37. The method of claim 35 wherein the step of allowing data to be written to a hard disk drive comprises the step of:

allowing data to be written to a file allocation table of the hard disk drive.

38. The method of claim 33 wherein the step of allowing execution of the interface control command further comprises the step of:

allowing data to be written to a floppy disk drive.

39. The method of claim 33 wherein the step of allowing execution of the interface control command further comprises the step of:

allowing data to be written to a BIOS memory.

40. The method of claim 33 wherein the step of allowing execution of the interface control command further comprises the step of:

allowing data to be written to a parallel port.

41. The method of claim 33 wherein the step of allowing execution of the interface control command further comprises the step of:

allowing data to be written to a serial port.

42. The method of claim 41 wherein the step of allowing data to be written to a serial port further comprises the step of:

allowing data to be written to a universal serial bus (USB).

43. The method of claim 41 wherein the step of allowing data to be written to a serial port further comprises the step of:

allowing data to be written to an IEEE-1394 interface.

44. The method of claim 33 wherein the step of allowing execution of the interface control command further comprises the step of:

allowing data to be written to a flash memory device.

45. The method of claim 33 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command is a hard disk drive formatting command.

46. The method of claim 45 wherein the step of determining whether the interface control command is the hard disk drive formatting command further comprises the step of:

determining whether the interface control command is a boot sector write command.

47. The method of claim 33 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command is a program file write command.

48. The method of claim 47 wherein the step of determining whether the interface control command is a program file write command further comprises the steps of:

obtaining a file extension from the interface control command;

determining whether the file extension is an executable file extension.

49. The method of claim 48 wherein the step of determining whether the file extension is an executable file extension further comprises the step of:

determining whether the file extension is one of a exe extension, a com extension, a bat extension, or a bin extension.

50. The method of claim 33 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command changes a file attribute, the file attribute enabling or disabling execution of a file corresponding to the file attribute.

51. The method of claim 33 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command disables a thermal management subsystem.

52. The method of claim 51 wherein the step of determining whether the interface control command disables a thermal management subsystem comprises the step of:

determining whether the interface control command disables a fan.

53. The method of claim 33 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command is a write command to write to system firmware (BIOS).

54. The method of claim 33 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command is a write command to write to a parallel port.

55. The method of claim 33 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command is a write command to write to a serial port.

56. The method of claim 55 wherein the step of determining whether the interface control command is a write command to write to a serial port comprises the step of:

determining whether the interface control command is a write command to write to a universal serial bus (USB).

57. The method of claim 55 wherein the step of determining whether the interface control command is a write command to write to a serial port comprises the step of:

determining whether the interface control command is a write command to write to an IEEE-1394 interface.

58. The method of claim 33 wherein the step of determining whether the interface control command introduces a security risk comprises the step of:

determining whether the interface control command is a write command to write to a flash memory device.

59. The method of claim 33 wherein the step of determining whether the source of the interface control command is authentic comprises the step of:

issuing a challenge to the source of the interface control command;

receiving a response from the source of the interface control command; and

determining whether the response is valid.

60. The method of claim 59 wherein the step of determining whether the response is valid comprises the step of:

comparing the response to a mathematical function of a value accessible only to the protection engine and to an operating system.

61. The method of claim 60 further comprising the step of:

writing the value from a processor to a one-time-writable register in the protection engine (by an operating system) during a boot process (before application software is enabled).

62. The method of claim 59 wherein the step of determining whether the response is valid comprises the step of:

performing a mathematical operation on the challenge to produce a correct response value; and

comparing the response to the correct response value.

63. The method of claim 59 wherein the step of issuing the challenge to the source of the interface control command includes the step of:

obtaining a pseudorandom value; and

forming the challenge based on the pseudorandom value.

64. Apparatus for protection of computer assets from unauthorized access comprising:

an interface controller operatively coupled to receive a interface control command to control an interface device;

a switch selectable between a protected state and an unprotected state;

a protection engine operatively coupled to the interface controller to receive the interface control command and operatively coupled to the switch to detect whether the electrical switch is in the protected state or the unprotected state to determine whether the interface control command poses a security risk and to selectively inhibit or allow execution of the interface control command by the interface controller depending on whether or not the interface control command poses the security risk and depending on whether the switch is in the protected state or the unprotected state.

65. The apparatus of claim 64 further comprising:

a timer operatively coupled to the switch to reset the switch to the protected state after a period of time has elapsed.

66. The apparatus of claim 64 further comprising:

an interface control command execution completion sensor operatively coupled to the switch to reset the switch to the protected state after an execution of the interface control command has been completed.

67. Apparatus for protection of computer assets from unauthorized access comprising:

an interface controller operatively coupled to receive a interface control command to control an interface device;

a protection engine operatively coupled to the interface controller for preventing unauthorized access to the interface device and operatively coupled to receive the interface control command to determine whether a source of the interface control command is authentic and to selectively allow or inhibit execution of the interface control command by the interface controller depending on whether or not the source of the interface control command is authentic.

68. The apparatus of claim 67 further comprising:

a one-time-writable register operatively coupled to the protection engine to store a value used to determine whether the source of the interface control command is authentic.

69. The apparatus of claim 68 wherein the value is accessible only to the protection engine and to an operating system.